National Cyber Security Centre
a part of GCHQ

Report (/)

Weekly Threat Report 16th February 2018

Created: 16 Feb 2018
Updated: 16 Feb 2018

This report is drawn from recent open source reporting.

Cryptocurrency mining update

On 11 February 2018, the NCSC made a statement(/news/ncsc-statement-malware-being-used-illegally-mine-cryptocurrency) to reassure the public that, whilst some government websites had been affected by malware designed to illegally mine cryptocurrency, no one was at risk of having their money stolen. The only possible effect on users' machines was reduced performance.

The NCSC then followed up with guidance(/guidance/ncsc-advice-malicious-software-used-illegally-mine-cryptocurrency) detailing how a compromised third party JavaScript library called Browsealoud had caused visitors to websites with the library embedded inadvertently to run mining code for the attackers. This would have caused no effect other than using up the device's CPU power. The compromise was mitigated easily by Browsealoud being taken offline by their administrators.

For more on cryptocurrency mining, see last week's NCSC Threat Report (published 9 February 2018)(/report/weekly-threat-report-9th-february-2018).

Domain name hijacking on managed services provider

Domain hijacking is a form of theft where the attacker takes control of a domain name without the consent of the original registrant. Hijacking can happen because of security flaws or due to the domain name's rental period expiring. Last week, a major US managed services provider had three of its domain names hijacked, shutting off email and websites for many of the company's clients. The company hosts more than 100,000 websites and 40,000 managed technology accounts, mostly for small and medium-sized enterprises (SMEs).

After taking control of the domain names, the hacker replaced the customer login page with a web chat service. Customers were then tricked into chatting to the perpetrator instead of being able to access their control panel.

Assessment

Domain hijacking has been a problem for many years, but this is likely to be one of the largest in terms of scale of websites potentially affected. However, it is highly unlikely that this particular domain hijacking significantly affected UK organisations. It is currently unknown how the domain names were hijacked but it is likely the domains simply expired, allowing the hackers to re-register them.

Domain hijacking could potentially have significant negative implications for any company/organisation that has a web presence. Attackers could replace a company's website, or web application, with an identical replica site designed to trick visitors into entering login credentials or personal information, thereby potentially helping to facilitate fraud. Malicious software could also be uploaded onto visitors' computers. If a hijacked domain had been whitelisted by other businesses, that trust would be extended to the attacker. Such actions would almost certainly cause significant reputational as well as financial damage to affected organisations. Managed service providers are likely to be a higher priority target of domain hijacking due to the potential access and damage they could cause to their clients.

Organisations can protect themselves against domain hijacking in several ways, including:

- Locking the domain using a web service to guard against unauthorised domain transfers
- Ensuring all of domain name contacts have valid contact information
- Setting the domain to auto-renew each year

Cryptocurrencies on the Darknet

According to the threat intelligence company Recorded Future, cryptocurrencies such as Litecoin and Dash are threatening to replace Bitcoin as the most used payment methods in online criminal marketplaces. This appears to be driven by relatively high Bitcoin payment fees, especially for smaller transactions, and delays in completing purchases due to the adopted three confirmations rule. This rule, to combat double-spending abuse, sees most vendors on the Darknet require three published confirmations to the blockchain before treating transactions as complete.

The researchers say that the prospect of waiting up to 24 hours to confirm some transactions, coupled with payment fees that could amount to 30% of the transaction value, is rendering Bitcoin unattractive for a large number of cyber criminals. The technology behind Litecoin is very similar to Bitcoin but it allows for faster transactions and significantly lower commission fees, resulting in an increasing number of vendors accepting it and other easier-to-use cryptocurrencies as payment.

Recorded Future expect the cryptocurrency diversification trend to intensify and suggest that Bitcoin might lose its dominant position among payment methods on the Darknet in the next six to twelve months, although it is still likely to remain one of the main payment instruments. More widely, legitimate users of cryptocurrencies are likely to take the same factors into account, and cryptocurrencies that are the quickest, easiest and cheapest to use are most likely to succeed.

FCA and ICO publish joint update on GDPR

Designed to improve the security of personal data, the EU's General Data Protection Regulation (GDPR) will apply to all organisations that process personal data, including the financial services industry, from 25 May 2018. Some organisations are already required to notify the Information Commissioner's Office (ICO), and possibly some other bodies, when they suffer a breach of personal data. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO and, in some cases, to individuals. Organisations will have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals. Failure to report a breach when required to do so could result in a significant fine of up to 2% of an organisation's annual turnover, or €10 million, as well as a fine for the breach itself.

Following feedback from industry, the Financial Conduct Authority (FCA) has published a joint update (https://www.fca.org.uk/news/statements/fca-and-ico-publish-joint-update-gdpr) with the ICO (with whom they have been closely working in preparation for GDPR). This update reassures firms that the GDPR does not impose requirements that are incompatible with the FCA handbook and highlights that, in fact, many of these GDPR requirements are directly compatible with the FCA handbook itself. They also re-emphasise that compliance with GDPR is a board-level responsibility and that they must be able to demonstrate the actions they have taken to ensure compliance.

This update follows a report last month from the Department for Digital, Culture, Media and Sport (DCMS) urging organisations to prepare as, worryingly, DCMS data showed that fewer than half of all businesses and charities were even aware of GDPR.

--

Topics

Cyber threats(/topics/cyber-threats)
Cyber attacks(/topics/cyber-attacks)
Vulnerabilities(/topics/vulnerabilities)

Was this report helpful?

We need your feedback to improve this content.

Yes No